EUCC Certification Report

TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0

Sponsor and Developer:	***Tongxin Microelectronics Co., Ltd*** **F/1, Building B-1, Zhongguancun Dongsheng Technology Park Northern Territory, NO.66 Xixiaokou Road, Haidian District, Beijing** **China**
Evaluation facility:	***Applus+ Laboratories*** **Campus UAB – Ronda de la Font del Carme, s/n 08193, Bellaterra, Barcelona, Spain**
Report number:	**EUCC-3110-2026-2500080-01 Certification Report**
Report version:	1
Project number:	**EUCC-2500080-01**
Author(s):	**Jordi Mujal, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**18 September 2026**
Number of pages:	**18**
Number of appendices:	**0**

Reproduction of this report is authorised only if reproduced in its entirety.

® TrustCB is a registered trademark. Any use or application requires prior approval by TrustCB.

CONTENTS

Foreword 3

International recognition of the certificate 4

1 Executive Summary 5

2 ICT Product details 7

2.1 Identification of the ICT Product 7
2.2 Contact information related to the evaluation of the ICT Product 7
2.3 Security services and policies 8
2.3.1 Security services 8
2.3.2 Vulnerability management 8
2.3.3 Assurance Continuity policies 8
2.3.4 Lifecycle management processes and production facilities 8
2.3.5 Patch management process 8
2.4 Assumptions and Clarification of Scope 8
2.4.1 Assumptions 8
2.4.2 Clarification of scope 8
2.5 Architectural Information 9
2.6 Supplementary Cybersecurity Information 9

3 Evaluation summary 11

3.1 Identification of used assurance components 11
3.2 EUCC State of the Art documents and Protection Profiles 11
3.3 ICT Product testing 11
3.3.1 Testing approach and depth 11
3.3.2 Independent penetration testing 11
3.3.3 Test configuration 11
3.3.4 Test results 11
3.4 ICT Product evaluation 12
3.4.1 Reused evaluation results 12
3.4.2 Evaluated configuration 12
3.4.3 Assessment against each assurance requirement 12
3.5 Results of the evaluation 14
3.6 Certificate information and scheme label 14
3.7 Comments and Recommendations 14

4 Security Target 16

5 Glossary 16

6 Bibliography 17

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

Reproduction of this report is authorised only if it is reproduced in its entirety.

International recognition of the certificate

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0, identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is Tongxin Microelectronics Co., Ltd located in Beijing, China and they also act as the sponsor of the evaluation and certification.

This Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the ICT product for their particular requirements.

The TOE is the dual interface integrated circuit chip of machine-readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control and Active Authentication according to the *[PP]*. The ICAO application is programmed on top of a JavaCard Platform without post-issuance loading application capacity.

The TOE claims conformance to the following Protection Profile *[PP]*:

- Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control (MRTD-PP), Version 1.10, 25 March 2009, registered under the reference BSI-CC-PP-0055-2009

Organisational Security Policies for the ICT product are stated to be the same as in the *[PP]*. No items have been added, removed or modified. Threats are presented in Section 3.3 of *[ST]* and include the threats as presented in the *[PP]*, and also includes additional threats.

A certification procedure was conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate, The certificate identifier is **EUCC-3110-2026-2500080-01**, dated **18 September 2026** and with a 5-year validity.

The evaluation of the TOE was performed by Applus+ Laboratories located in Barcelona, Spain. The evaluation was completed on 20-08-2026 with the issuance of the evaluation technical report *[ETR]*. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, R1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 R1 *[CC]* (Parts 1, 2, 3, 4, 5).

The scope of the evaluation was defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ADV_FSP.5 (Complete semi-formal functional specification with additional error information), ADV_INT.2 (Well-structured internals), ADV_TDS.4 (Semi-formal modular design), ALC_CMS.5 (Development tools CM coverage), ALC_DVS.2 (Sufficiency of security measures), ALC_FLR.1 (Basic flaw remediation), ALC_TAT.2 (Compliance with implementation standards) and ATE_DPT.3 (Testing: modular design). The AVA_VAN level applied during the evaluation was AVA_VAN.3.

This assurance level is recognised by article 52 of [CSA] as 'high'.

The TOE also claims the assurance Composite product package as defined in *[CC]* (Part 5).

Consumers of this ICT Product are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

---

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

Note that the certification results apply only to the specific version of the product as evaluated.

2 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0 from Tongxin Microelectronics Co., Ltd located in Beijing, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	THD89 1.0	1.0
Firmware	Crypto Library	1.01
	CryptoECCSec library	1.20
	tmcRSA_ECC_DH_SHA_SecurityLib Library	5.09
	Boot code	1.0
Software	TMCICAO Application	1.0
	TMCOS	4.0 0.5
Key	Root keys-IMK	1.0
	Root keys-TEK	1.0

Additional requirements for the operational environment of the certified ICT product are described in section 4.2 of the *[ST]*.

To ensure secure usage a set of guidance documents is provided with the TOE. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate

Organisation name:	Tongxin Microelectronics Co., Ltd
Address:	F/1, Building B-1, Zhongguancun Dongsheng Technology Park Northern Territory, NO.66 Xixiaokou Road, Haidian District, Beijing, China
Certified product contact details	liuchao@tsinghuaic.com

Developer of the certified ICT Product

Organisation name:	Tongxin Microelectronics Co., Ltd
Address:	F/1, Building B-1, Zhongguancun Dongsheng Technology Park Northern Territory, NO.66 Xixiaokou Road, Haidian District, Beijing, China
Certified product contact	liuchao@tsinghuaic.com
Website link for supplementary cybersecurity information associated with the TOE, in accordance with Article 55 of [EU-EUCC]	https://www.tsinghuaic.com/index/index/newsdetial/id/608?lang=en

Identification of CAB

The Certification Assessment Body for this ICT Product is TrustCB B.V located in Hoofddorp, The Netherlands.

Identification of ITSEF

Evaluation and testing for this ICT Product was performed by following ITSEF:

Applus+ Laboratories located in Barcelona, Spain.

Responsible national cybersecurity certification authority

Dutch Authority for Digital Infrastructure (RDI)

2.3 Security services and policies

2.3.1 Security services

These are the main TOE features as described in the *[ST]*: The TOE is a dual interface integrated circuit chip of machine-readable travel documents (MRTD's chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control and Active Authentication according to the International Civil Aviation Organization (ICAO).

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0

Document reference: EUCC Security Vulnerability Management Procedure, version A.

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

Not applicable to this evaluation.

2.3.5 Patch management process

Not applicable to this evaluation.

2.4 Assumptions and Clarification of Scope

2.4.1 Assumptions

As per the *[ST]* conformance claim rationale, all the assumptions defined in the claimed *[PP]* are taken.

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions described in the [ST]. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

2.4.2 Clarification of scope

Considering all Assumptions above, the evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

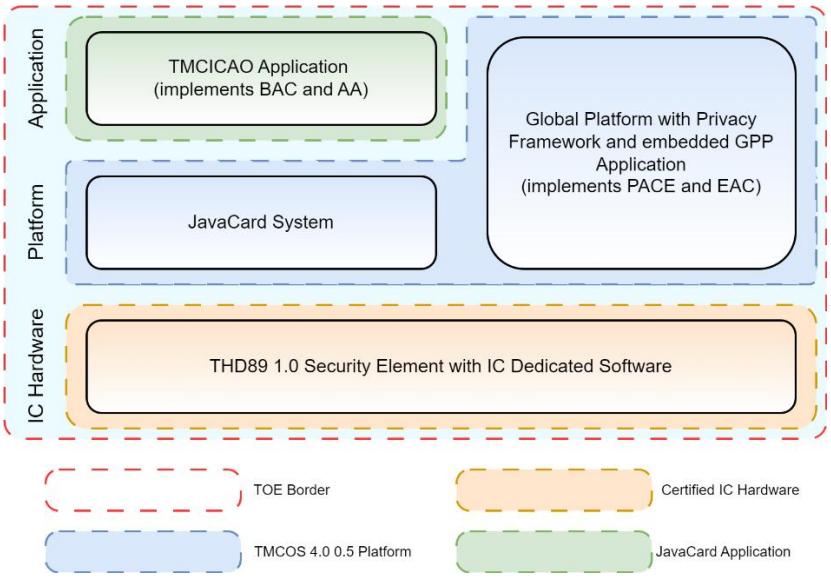
Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

The environment in which the TOE is personalised must perform proper and safe personalisation according to the guidance and referred ICAO guidelines.

The environment in which the TOE is used must ensure that the inspection system protects the confidentiality and integrity of the data send and read from the TOE.

2.5 Architectural Information

The top-level block diagram of the TOE as it is depicted in the *[ST]*:



2.6 Supplementary Cybersecurity Information

The following website link was provided for the TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

https://www.tsinghuaic.com/index/index/newsdetial/id/608?lang=en

This link provides further details and links on:

- Guidance and recommendations to assist end users of the TOE with the secure configuration, installation, deployment, operation and maintenance of the TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0.
- The period during which the TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0 security support will be offered to end users of the TOE, in particular as regards the availability of cybersecurity related updates, is stated as 5 years, aligned with the validity of the issued EUCC certificate.
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0.
- the online repository listing publicly disclosed vulnerabilities related to the TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0 and to any relevant cybersecurity advisories .

The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0:

Identifier	**Version**
TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Operational User Guidance	v0.7
TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Preparative procedures	v0.6
TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Personalization Guidance	v0.6
TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Pre-Personalization Guidance	v0.6

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.2 and ATE_DPT.3** and
- **Composition evaluation package (COMP)**,

as defined by, and detailed in, *[CC]* and *[CEM]*.

3.2 EUCC State of the Art documents and Protection Profiles

EUCC state-of-the-art documents *[SotA Documents]* were applied as referenced in the Bibliography.

The following Protection Profiles were applied:

Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (MRTD-PP), as certified under the reference BSI-CC-PP-0055-2009 by CAB Bundesamt für Sicherheit in der Informationstechnik (BSI), following evaluation by SRC & Consulting GmbH. The author of this Protection Profile is the CAB Bundesamt für Sicherheit in der Informationstechnik (BSI). The assurance package required for a product conforming to this protection profile is EAL4 augmented with ALC_DVS.2.

3.3 ICT Product testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

3.3.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and SFR-enforcing module level. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

3.3.2 Independent penetration testing

The independent vulnerability analysis performed was conducted along the steps described in section 3.4.3, AVA part.

3.3.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

3.3.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

3.4 ICT Product evaluation

The evaluation was performed referencing ISO/IEC 18045, Common Evaluation Methodology, and the EUCC State of the Art documents listed in section 6 of this report as *SotA* Documents.

Further security evaluation criteria were not applied in this evaluation.

3.4.1 Reused evaluation results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of multiple site certificates and Site Technical Audit Reports.

3.4.2 Evaluated configuration

The TOE is defined uniquely by its name and version number TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0.

3.4.3 Assessment against each assurance requirement

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2
TOE summary specification	ASE.TSS.1
Consistency of Composite product ST	ASE.COMP.1

The *[ST]* document contains all the necessary information to fulfil with the requirements defined for the evaluation of ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.2, ASE_ECD.1, ASE_REQ.2, ASE_TSS.1 and ASE_COMP.1 families.

All the families have obtained a pass verdict and all dependencies have been fulfilled. Therefore, the assignation of a PASS verdict for ASE class is justified.

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.5
Implementation representation	ADV_IMP.1
TSF Internals	ADV_INT.2
TOE design	ADV_TDS.4
Composite design compliance	ADV_COMP.1

The ADV evidence provided by the developer contains all the necessary information to fulfil with the requirements defined for the evaluation of ADV_ARC.1, ADV_FSP.5, ADV_IMP.1, ADV_INT.1, ADV_TDS.4 and ADV_COMP.1 families. The information regarding TOE architecture, TSFIs, modules, subsystems, TOE implementation representation and TSF internals is consistent, complete and accurate for the evaluation level.

All the families have obtained a pass verdict and all dependencies have been fulfilled. Therefore, the assignation of a PASS verdict for ADV class is justified.

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

The TOE and its guidance contain all the necessary information to fulfil with the requirements defined for the evaluation of AGD_OPE.1 and AGD_PRE.1. The information regarding TOE operational user guidance and TOE acceptance procedure is clear, consistent, and reasonable.

All the families have obtained a pass verdict and all dependencies have been fulfilled. Therefore, the assignation of a PASS verdict for AGD class is justified.

ALC

ALC	
CM capabilities	ALC_CMC.4
CM Scope	ALC_CMS.5
Delivery	ALC_DEL.1
Development security	ALC_DVS.2
Life cycle definition	ALC_LCD.1
Flaw remediation	ALC_FLR.1
Tools and techniques	ALC_TAT.2
Integration of composition parts and consistency check of delivery procedures	ALC_COMP.1

The ALC evidence and the STARs of each site involved in the TOE life cycle provide all the necessary information to fulfil with the requirements defined for the evaluation of ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2, ALC_FLR.1 and ADV_COMP.1. The information regarding configuration management capabilities, configuration management scope, TOE delivery, development security, TOE life cycle definition, development tools and techniques, and flaw remediation is consistent, complete and accurate for the evaluation level.

All the families have obtained a pass verdict and all dependencies have been fulfilled. Therefore, the assignation of a PASS verdict for ALC class is justified.

ATE

ATE	
Coverage	ATE_COV.2
Depth	ATE_DPT.3
Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2
Composite functional testing	ATE_COMP.1

The developer test documentation contains all the necessary information to fulfil with the requirements defined for the evaluation of ATE_COV.2, ATE_DPT.3, ATE_FUN, ATE_IND.2 and ATE_COMP.1 families. The information regarding developer testing, coverage between tests, TSFIs, modules,

subsystems, modules/subsystem interactions is complete, consistent, and accurate for the evaluation level. Furthermore, during the witnessing session and the laboratory independent test plan, the sample configuration used is the same as the one defined in the security target.

All the families have obtained a pass verdict and all dependencies have been fulfilled. Therefore, the assignation of a PASS verdict for ALC class is justified.

AVA

AVA	
Vulnerability analysis	AVA_VAN.3
Composite vulnerability assessment	AVA_COMP.1

A vulnerability analysis was performed and penetration tests based on the vulnerability analysis were conducted. No deviation from the expected result was detected. Therefore, the TOE meets the requirements defined for the evaluation of AVA_VAN.3 and AVA_COMP.1 families. *[SotA_AAPS]* was used during the analysis.

All the families have obtained a pass verdict and all dependencies have been fulfilled. Therefore, the assignation of a PASS verdict for AVA class is justified.

3.5 Results of the evaluation

Based on the above evaluation results the evaluation lab concluded the TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration, version 1.0, to be **CC:2022 R1 1 Part 2 extended, CC:2022 R1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as 'high' and to meet the requirements of **EAL 4 augmented with ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.2 and ATE_DPT.3**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

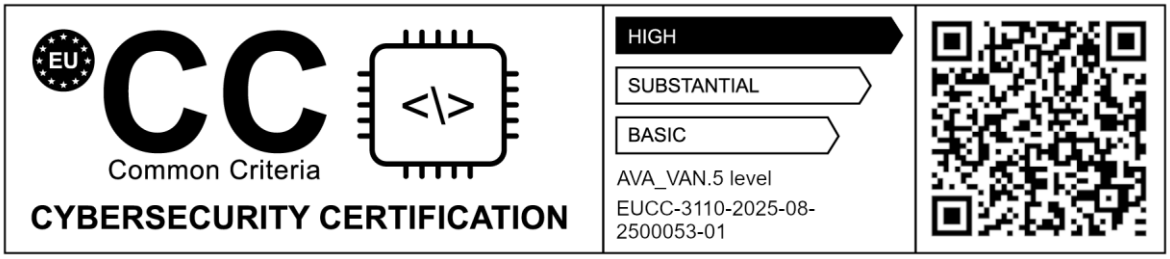
The Security Target claims 'strict' conformance to the Protection Profile *[PP]*.

3.6 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2026-2500080-01

Date of issuance: 18 September 2026 and with a validity period of **5 years**.



3.7 Comments and Recommendations

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

4 Security Target

The certification references the following security target:

TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Security Target, version v1.2, 15 July 2026 *[ST]*.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

5 Glossary

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

BAC	Basic Access Control
EAC	Extended Access Control
eMRTD	electronic MRTD
ICAO	International Civil Aviation Organization
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MRTD	Machine Readable Travel Document
NSCIB	Netherlands Scheme for Certification in the area of IT security
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
TOE	Target of Evaluation

6 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, CC:2022 Parts 1, 2, 3, 4 and 5, R1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 R1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2
[CC2022_TP]	Transition Policy to CC:2022 and CEM:2022
[DEV_DOCS]	TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Operational User Guidance, v0.7 TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Preparative procedures, v0.6 TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Personalization Guidance, v0.6 TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Pre-Personalization Guidance, v0.6 TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC and EAC with PACE configuration CM Scope, v1.2
[ETR]	Evaluation Technical Report, CNLTMC002-ETR-M5, version M5, 20 August 2026
[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[EU-EUCC-amdt.1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EU-EUCC-amdt.2]	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents
[HW-CERT]	CERTIFICATION REPORT, 2023-33-INF-4571- v1, Issued by CCN, 15 July 2025
[HW-ETRfC]	ETR for Composite Evaluation, THD89 Secure Microcontroller version 1.0, CCETMC002R1-ETRfC-M1, version M1, Applus Laboratories, 03 June 2025
[HW-ST]	THD89 Secure Microcontroller version 1.0 Security Target Lite. version 1.0, April 2025
[PP]	Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (MRTD-PP), Version 1.10, 25 March 2009, registered under the reference BSI-CC-PP-0055-2009

[SotA_AAPS]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Application of Attack Potential to Smartcards and Similar Devices, Version 2, February 2025
[SotA_COMP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Composite product evaluation and certification for CC: 2022 Version 1, February 2025
[SotA_MSSR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Minimum Site Security Requirements, Version 2, February 2025
[SotA_SARC]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, version 1.1, October 2023
[SotA_STAR]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT, STAR methodology, version 1, February 2025
[ST]	TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Security Target, version v1.2, 15 July 2026
[ST-lite]	TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration Security Target Lite, version v1.1, 17 April 2026
[ST-SAN]	Sanitization of a security target for publication, [EUCC] Annex V section V.2 ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)